CLOUD SECURITY POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	CLOUD SECURITY POLICY
Document Number:	COS/POL/13
Version:	1.0
Document Date:	17-06-2026
Prepared By:	HOD-IT
Reviewed By:	CISO
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Review Date	Version No.
1	Initial Basic Release	**17-06-2026**	1.0

Contents

1. PURPOSE

The purpose of this Policy is to establish a secure governance framework for the adoption, implementation, and management of cloud computing services at LLP. It aims to protect organizational information and cloud-based assets against unauthorized access, misuse, disclosure, alteration, loss, or disruption while ensuring compliance with applicable legal, regulatory, contractual, and business requirements.

2. SCOPE

- This Policy applies to all cloud services, applications, infrastructure, storage environments, users, employees, consultants, contractors, third-party service providers, and business partners who access, manage, or process information on behalf of LLP using cloud technologies.
- The Policy covers Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), public, private, hybrid, and multi-cloud environments used by the organization.

3. POLICY STATEMENT

A) Cloud Governance

All cloud services shall be approved by management before implementation. Cloud adoption shall be based on business requirements, risk assessment, data sensitivity, regulatory obligations, and security considerations. Appropriate ownership shall be assigned for every cloud resource and service.

B) Shared Responsibility

LLP and the Cloud Service Provider shall clearly understand and document their respective security responsibilities. While infrastructure protection may be managed by the provider depending on the deployment model, LLP shall remain responsible for protecting organizational data, user identities, access controls, and regulatory compliance.

C) Risk Assessment and Vendor Management

Cloud service providers shall undergo appropriate due diligence before engagement. The evaluation shall consider security controls, certifications, compliance obligations, service availability, privacy practices, disaster recovery capabilities, contractual commitments, and incident response arrangements. Vendor performance shall be reviewed periodically throughout the service lifecycle.

D) Asset and Data Protection

All cloud-hosted information shall be classified according to its sensitivity and protected using appropriate security controls. Sensitive information shall be encrypted during storage and transmission wherever applicable. Backup, retention, and secure disposal of organizational information shall be performed in accordance with approved business and legal requirements.

E) Identity and Access Management

Access to cloud resources shall be granted strictly on the basis of business need and the Principle of Least Privilege. Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), strong authentication mechanisms, and periodic access reviews shall be implemented to protect cloud environments. Privileged activities shall be monitored and logged.

F) Infrastructure and Network Security

Cloud infrastructure shall be securely configured using approved security standards. Firewalls, network segmentation, intrusion detection and prevention mechanisms, secure remote connectivity, malware protection, vulnerability management, and timely security patching shall be implemented to safeguard cloud resources against cyber threats.

G) Secure Configuration and Change Management

Cloud resources shall be deployed using approved secure configuration standards. All significant changes to cloud infrastructure or services shall undergo formal change management, including risk assessment, testing, authorization, documentation, and post-implementation review to minimize operational and security risks.

H) Application Security

Applications hosted in cloud environments shall follow secure development practices throughout their lifecycle. Security testing, vulnerability assessments, secure coding standards, API protection, and periodic penetration testing shall be performed to reduce application security risks and improve resilience against cyber threats.

I) Logging, Monitoring and Security Operations

Cloud environments shall generate and retain security logs sufficient to support operational monitoring, incident detection, forensic investigations, and regulatory compliance. Security events shall be continuously monitored using appropriate monitoring tools, with alerts investigated and escalated in accordance with the organization's incident management procedures.

J) Backup, Business Continuity and Disaster Recovery

Business-critical cloud information shall be backed up regularly and protected against accidental loss or corruption. Recovery procedures shall be tested periodically to verify data integrity and restoration capability. Business continuity and disaster recovery arrangements shall support timely recovery of critical cloud services.

K) Incident Management

All actual or suspected cloud security incidents shall be reported immediately through the established incident reporting process. Security incidents shall be investigated, documented, contained, and resolved in a timely manner. Root cause analysis and corrective actions shall be implemented to prevent recurrence.

L) Compliance

Cloud services shall comply with applicable legal, regulatory, contractual, and information security requirements. Periodic reviews, internal assessments, vulnerability assessments, and independent audits shall be conducted to evaluate compliance with this Policy and identify opportunities for continual improvement.

M)Security Awareness

Employees and authorized users shall receive periodic awareness and training on cloud security responsibilities, secure use of cloud services, protection of organizational information, phishing awareness, incident reporting, and emerging cyber security threats.

4. ROLES AND RESPONSIBILITIES

Management shall provide oversight for cloud security governance and ensure adequate resources are available for implementing the Policy. Information Security and IT teams shall establish, monitor, and maintain cloud security controls. Cloud service owners shall ensure compliance within their respective services, while all users shall protect organizational information and comply with this Policy.

5. EXCEPTION MANAGEMENT

Any deviation from this Policy shall be formally documented, supported by a business justification, subjected to risk assessment, approved by authorized management, and periodically reviewed. Appropriate compensating controls shall be implemented wherever required.

6. POLICY REVIEW

This Policy shall be reviewed annually, or earlier where required due to changes in business operations, legal or regulatory obligations, cloud technologies, or information security risks.

7. NON-COMPLIANCE

Failure to comply with this Policy may result in disciplinary action, suspension of system access, contractual remedies, or legal action, as applicable under organizational policies and relevant laws.